



Australian Government



今すぐ行動して安全確保を

安全なネットの使用方法

やさしい文書版



このガイドの使用方法



私たちはオーストラリア政府の職員です。

私たちがこのガイドを書きました。



太文字で書いた言葉があります。

その言葉の意味を説明します。

28 ページには、言葉のリストもあります。



以下のことを信頼できる人に手伝ってもらえます：

- このガイドを読むこと
- もっと詳しい情報をみつけること



これは、ガイドの原文を読みやすいように要約したものです。

ですから、最も大切な内容だけを含んでいます。



原文は、このウェブサイトで見ることができます。

www.actnowstaysecure.gov.au

このガイドには何が書かれていますか。

このガイドについて	4
アカウントを安全に保つために	6
あなたの情報を守るために設定をチェック	10
あなたのデバイスを守る	16
詐欺	20
意見を言う	25
言葉のリスト	28
ご連絡ください	30

このガイドについて



私たち全員が、安全なネットの使用法について考えてみる必要があります。

これを**サイバーセーフティ**と言います。



サイバーとはインターネットに関連するもののことです。



このガイドでは、ネット上で自分を守る方法を説明します。

例えば、**サイバー犯罪**からです。

サイバー犯罪は、インターネットを使って行う犯罪です。



例えば、犯罪者は以下のことをするためにインターネットを使うかもしれません：

- あなたの個人情報を盗む
- あなたのオンラインアカウントやプロフィールを乗っ取る



サイバー犯罪はどんなデバイスにでも起こります。あなたの以下のデバイスも含まれます：

- コンピューター
- スマートフォン
- スマートウォッチ



サイバー犯罪から自分を守るためにできることがあります。



次のページからは、あなたができることについて説明します。

アカウントを安全に保つために



オンラインアカウントの安全な使用法について考えてみるべきです。

異なる強力なパスフレーズを使う



パスフレーズはより強力なパスワードです。

他人が推測するのは非常に難しいものです。



異なる強力なパスフレーズを使うことが、あなたのアカウントを守る上で、最善の方法の一つです。



それぞれのオンラインアカウントに、異なるパスフレーズを使うべきです。



強力なパスワードには、以下のものがあります：

- 4つ以上の無作為に並べた言葉
- 15以上の文字や数字



大文字を含むことができます。



以下のような記号も使えます：

- ダッシュ記号
- ドルの記号
- メールに使う記号の@



パスワードにあなたの個人情報を使ってはいけません。



例えば：

- あなたの誕生日
- あなたの家族やペットの名前

アカウントのログインに一手間追加



多要素認証(MFA)を使ってあなたのアカウントを守ることができます。

多要素認証は、アカウントにログインする度に、2種類以上の異なる認証方法を使います。



例えば、まずはパスワードを使わなければいけないかもしれません。

その後、あなたの携帯に受信するコードを入力します。

以下のものから選択できるかもしれません：



- あなたの携帯に入っているアプリでコードを受信する



- メールでコードを受信する



- テキストメッセージでコードを受信する



多要素認証は、他人があなたのオンラインアカウントに入りにくくするものです。

たとえばあなたのパスワードを探り当てたとしてもです。

あなたの情報を守るために設定をチェック



あなたのネット情報を守る設定になっているかをチェックすることができます。



これには以下の設定を含みます：

- オンラインアカウント
- デバイス
- アプリ



以下のことができます：

- 設定を変える
- あなたの情報を使えるアプリを選択する



デバイスの設定を見つけるには：

- 歯車のアイコンを探す

または

- デバイスの検索バーに「設定」と入力します



メニューを開くと、アプリやオンラインアカウントの設定が見つかるかもしれません。

横線が3本並んでいるように見えるものがメニューです。



設定によっては以下の情報をシェアすることができます：

- あなたが誰であるか
- あなたのいる場所
- あなたが住む場所



ネット上でそんな情報をシェアすると、サイバー犯罪にさらされるリスクがあります。



サイバー犯罪者が、あなたになりすましてあなたの情報を使うことができます。

犯罪者は以下の情報を使うかもしれません：



- あなたの住所



- あなたの家族の人の名前



- あなたのペットの名前



あなたを知っている人だけが、ソーシャルメディアプロフィールを見ることができるよう、アカウントを設定することができます。

例えば、あなたのフェイスブックプロフィールです。



この設定は、通常プライバシー設定と呼ばれています。



あなたの**位置情報の設定**をコントロールすることもできます。

位置情報の設定は、あなたのデバイスの位置を表示します。



位置情報の設定では、オンとオフの切り替え操作が可能です。

どのアプリがあなたの位置情報の設定を使うことができるかを選択することもできます。



以下のものに、この設定をすることができます：

- オンラインアカウント
- デバイス
- アプリ

以下のことができるかどうかをアプリが尋ねるかもしれません：



- あなたのカメラを使う



- あなたの写真を見る



あなたのカメラや写真を使えるのは、あなたがよく知っているアプリだけにして下さい。

あなたのデバイスを守る

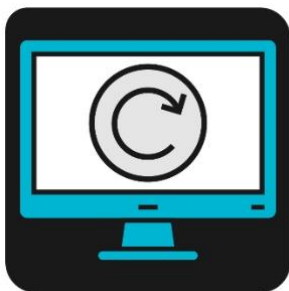


あなたのデバイスを守る方法について考えることが、オンラインでの安全を保つのに役立ちます。
例えば、あなたの携帯やスマートウォッチです。



これは、インターネットに接続するデバイスにとって重要です。

デバイスをアップデートする



オンライン上での安全を保つためにデバイスをアップデートすることができます。
例えば、あなたの携帯やノートパソコンです。



あなたのデバイスは、これをソフトウェアアップデートと呼ぶかもしれません。



アップデートは、サイバー犯罪からデバイスを守るのに役立ちます。



デバイスが、自動的にアップデートするよう設定することができます。



アップデートのし方についての詳細は、以下のウェブサイトを参照して下さい。

[www.actnowstaysecure.gov.au/
cyber-safe-actions](http://www.actnowstaysecure.gov.au/cyber-safe-actions)

公共の Wi-Fi ネットワーク



公共の Wi-Fi を使う時は、注意しなければいけません。



公共の Wi-Fi は、公共の場で使用できる無料の無線インターネットです。



例えば、以下の場所：

- カフェ
- 空港
- ホテル



公共の Wi-Fi を使ってウェブサイトに入れる情報には、気をつけなければいけません。



例えば、あなたの：

- 銀行の詳細
- メールアカウント
- ソーシャルメディアプロフィール



サイバー犯罪者は、以下のことをするために公共の Wi-Fi を使うことができます：

- ネット上であなたがしていることを見る
- あなたの情報を盗む

その理由は：



- 誰でも使うことができる



- 自分のデバイスを守るのが、より難しい



以下のウェブサイトで、公共の Wi-Fi の安全な使用法を学ぶことができます。

[www.actnowstaysecure.gov.au/
cyber-safe-actions](http://www.actnowstaysecure.gov.au/cyber-safe-actions)

詐欺



以下のことをするのを**詐欺**と呼びます：

- あなたを騙す
- あなたのお金を奪う



詐欺師は詐欺をする人のことです。

詐欺師は、こんなものを使って騙そうとするかもしれません：



- テキストメッセージや電話
- メール
- ソーシャルメディア
- ウェブサイト



詐欺師は、親切そうな人かもしれません。

でもあなたを騙して、あなたの情報を渡すよう仕向けるかもしれません。

詐欺師は、以下のことをするためにそれらを使うことができます：



- あなたのオンラインアカウントに侵入する



- あなたになりすます



- あなたの金銭を盗む

詐欺師は、こんなこともするかもしれません：



- あなたを騙すために、偽のアカウントを作る



- あなたがクリックするよう、リンクや広告をシェアする

詐欺の見分け方

以下のことがあれば、詐欺かもしれません：



- あなたに、すぐに何かをするよう頼む



- 多額の金銭を提供する



- 金銭をねだる



- リンクをクリックするよう頼む



詐欺師は、あなたが知っていて信頼する組織のふりをすることがあるかもしれません。

例えば、あなたの銀行です。



詐欺師は、あなたが個人情報をシェアしてくれることをあてにしてそんなことをするのです。



詐欺師だと思ったら、その人と話すのはやめて下さい。



本人が言う通りの人であるかどうかをチェックして下さい。

あなたが自分でみつけた信用できる連絡先を使って、その人や組織に連絡することができます。



もし何か変だと感じたら、自分を守るため、すぐに行動して下さい。

詐欺を報告する



Scamwatch は、オーストラリア人の味方です：

- 詐欺を理解する
- 詐欺を報告する



Scamwatch は、詐欺にあったオーストラリア人を助けてもくれます。



Scamwatch のウェブサイトには詐欺を報告することができます。

www.scamwatch.gov.au/report-a-scam

意見を言う



どうすればネット上で自分を守るかについて、はっきり意見を言うべきです。

これには以下のものがあります：



- サイバー犯罪を報告する



- あなたが知っていることを家族や友人とシェアする



以下に、はっきりと意見を言うことができる方法を説明します。

サイバー犯罪を報告する

サイバー犯罪の報告は、政府を助けてくれます：



- サイバー犯罪者がどのように人を攻撃しようとするかについて学ぶ



- より多くの人々を守る



サイバー犯罪を ReportCyber のウェブサイトにご報告することができます。

www.cyber.gov.au/report

家族や友人に安全なネットの使用方法について話す



家族や友人と安全なネットの使用方法についての秘訣をシェアする。

あなたも彼らから学ぶことができます。



安全なネットの使い方についての知識をシェアすることで、あなたやあなたの周りの人々を守ることができます。



他の人とデバイスをシェアしているのなら、その安全な使用方法について話すことも重要です。

言葉のリスト

これは、このガイドにある**太文字**の言葉の意味を説明するものです。



サイバー

サイバーとは、ネットに関連することです。

サイバー犯罪

サイバー犯罪は、犯罪者がネットを使って行う犯罪です。



例えば、以下のことをするためにネットを使うかもしれません：

- 個人情報を盗む
- オンラインアカウントを乗っ取る



位置情報の設定

位置情報の設定は、あなたのデバイスの位置を表示します。



多要素認証 (MFA)

多要素認証は、アカウントにログインする度に、2種類以上の異なる認証方法を使ってログインします。



パスワード

パスワードは、より強力なパスワードです。
他人が推測するのは非常に難しいものです。



公共の Wi-Fi

公共の Wi-Fi は、公共の場で使える無料の無線インターネットです。



詐欺

人が以下のことをしようとするのを詐欺と呼びます：

- あなたを騙す
- あなたの金銭を奪う



詐欺師

詐欺師は、詐欺をする人のことです。

ご連絡ください



Australian Cyber Security Hotline に電話することができます。

1300 292 371



以下のウェブサイトをご覧ください。

www.actnowstaysecure.gov.au



サイバー犯罪を ReportCyber のウェブサイト
に報告することができます。

www.cyber.gov.au/report



Information Access Group は、このやさしい文書を写真素材とカスタム画像を使って作成しました。この画像は許可なく再利用できません。この画像に関してのお問い合わせは、以下をご覧ください。

www.informationaccessgroup.com job number 6342 を付記して下さい。